SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY

COURSE NAME: 19OE201-Blockchain Technology

IV YEAR /VII SEMESTER

Unit II- CRYPTOCURRENCY

Topic : ZCASH

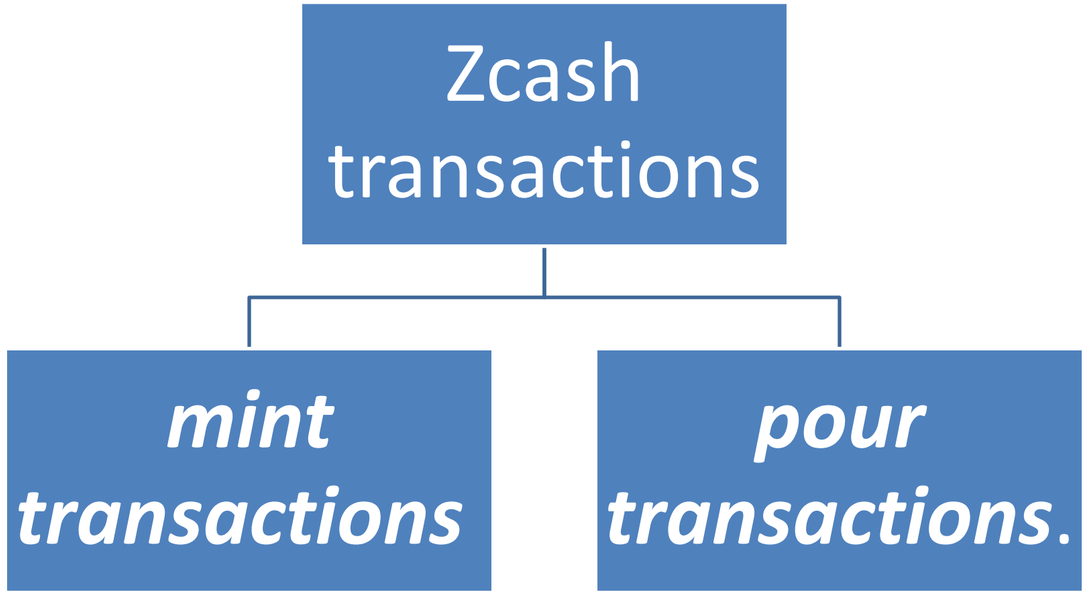
Zcash

- Zerocash is a protocol that provides a decentralized crypto-currency.
- It is being developed into a full-fledged digital currency- Zcash.
- It provides a *privacy-preserving* version of Bitcoin (or a similar currency).
- Bitcoin uses the hashing algorithm SHA-256.5CoinMarketCap. "SHA-256."
- ZCash uses Equihash, which is incompatible with hardware and software designed for Bitcoin mining.
- It also has larger blocks and increased hashing times, which increases the network's hash rate.

Mining Zcash

- ZCash uses the zk-SNARK security protocol to ensure the parties involved in a transaction are verified without revealing any information to each other or the network.
- ZCash uses proof-of-work and requires miners to compete against each other to produce a new block by racing to solve a cryptographic problem.
- The first miner to find the solution opens a new block and receives the block reward.

Transactions in Zcash



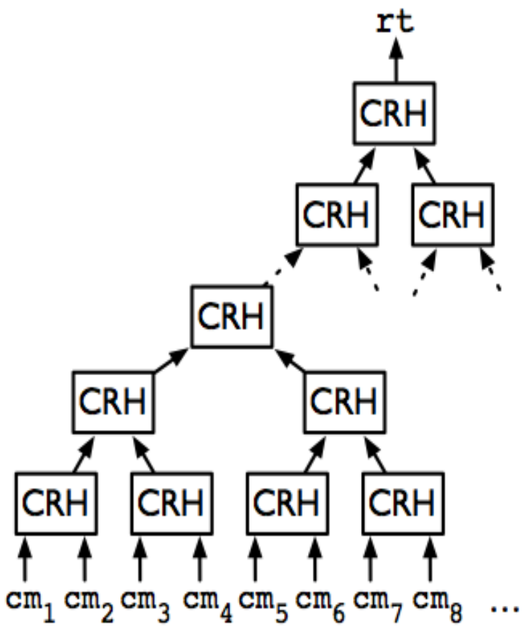
Mint Transactions in Zcash

Mint transactions.

- A mint transaction allows a user to convert a specified number of non-anonymous bitcoins (from some Bitcoin address) into the same number of zerocoins belonging to a specified Zerocash address.
- The mint transaction itself consists of a cryptographic commitment to a new coin, which specifies the coin's value, owner address, and (unique) serial number.
- The commitment is based on the SHA-256 hash function, and hides both the coin's value and owner address.

Transactions in Zcash

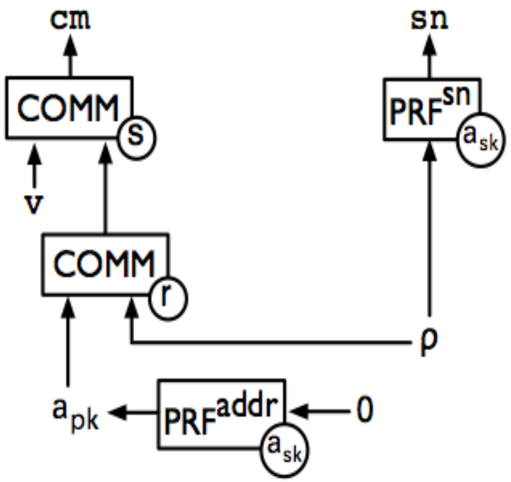
(a) Merke tree over $(cm_1, cm_2, \ldots)$



(b) coin

$$c = ((a_{pk}, pk_{enc}), v, \rho, r, s, cm)$$

(c) coin commitment (d) serial number



`rt` = *Merkle-tree root*
`cm` = *coin commitment*
`sn` = *serial number*
`v` = *coin value*
`r, s` = *commitment rand.*
ρ = *serial number rand.*
(a_{pk}, pk_{enc}) = *address public key*
(a_{sk}, sk_{enc}) = *address secret key*

Pour Transactions in Zcash

Pour transactions.

- A pour transaction allows a user to make a private payment, by consuming some number of coins (owned by this user) in order to produce new coins.
- Ex:., a pour transaction, for (up to) two input coins and (up to) two output coins, involves proving, in zero knowledge, that:
  - the user owns the two input coins;
  - each one of the input coins appears in some previous mint transaction or as the output coin of some previous pour transaction; and
  - the total value of the input coins equals the total value of the output coins.

References

TEXT BOOKS

1. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas M Antonopoulos 2018
2. Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.
3. https://101blockchains.com/blockchain-vs-database-the-difference/

REFERENCES

1. William Mougayar, “Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.
2. Josh Thompson, ‘Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming’, Create Space Independent Publishing Platform, 2017.
3. Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, July 19, 2016.
4. Henning Diedrich, Ethereum: Block chains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations-2016

Thank You